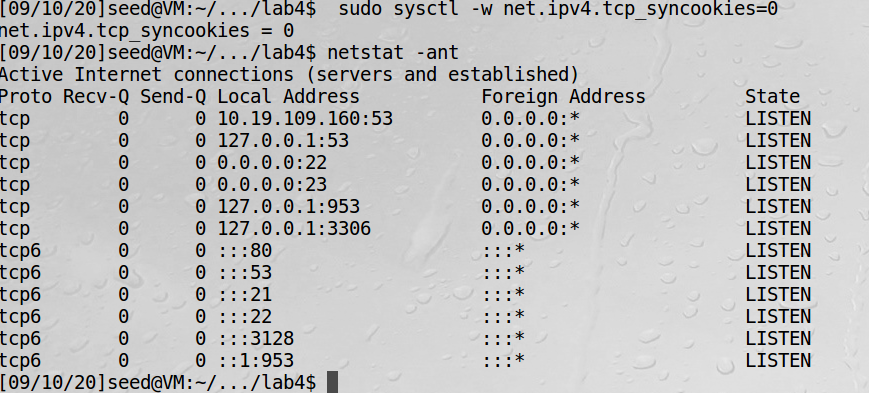
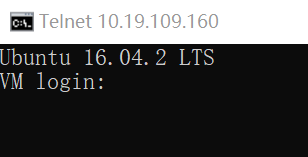
# TCP/IP Attack Lab

## 3.1 Task 1: SYN Flooding Attack



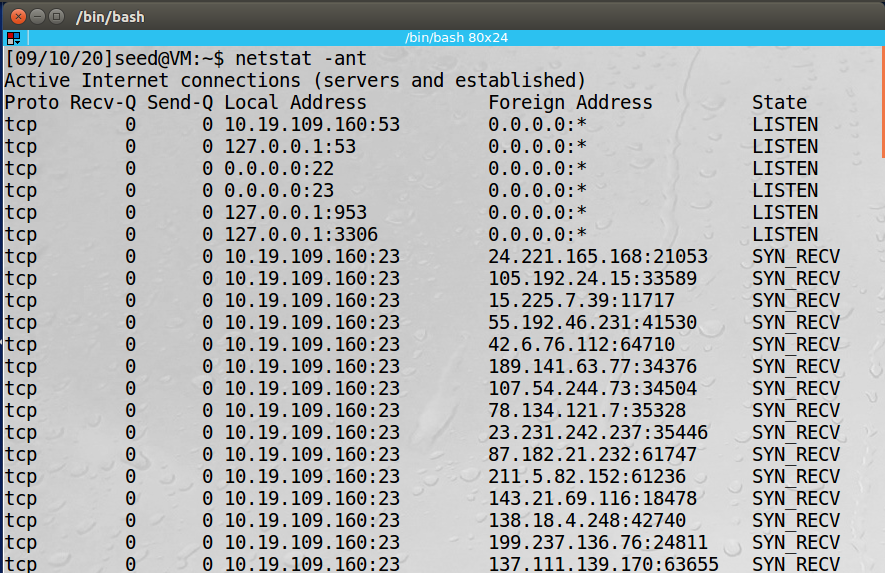
在服务器上关闭SYN cookie并检查半开放连接数

在宿主机上远程登录虚拟机10.19.109.160

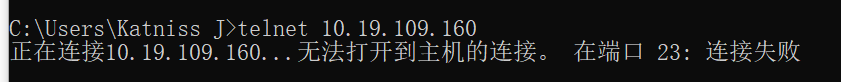


实施攻击





受到泛洪攻击



从宿主机上无法登录

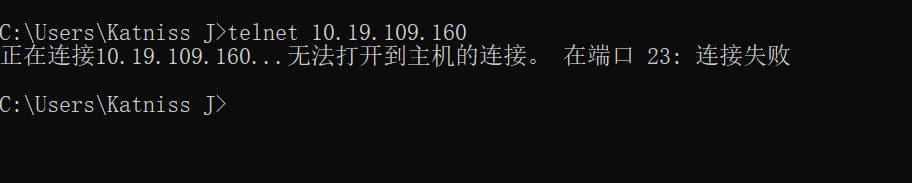
## 3.2 Task 2: TCP RST Attacks on telnet and ssh Connections

远程登录建立连接



使用netwox 78进行攻击

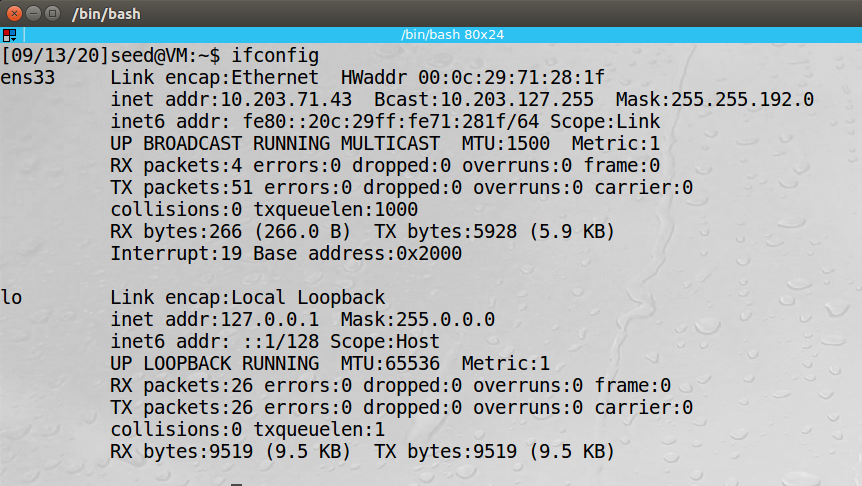




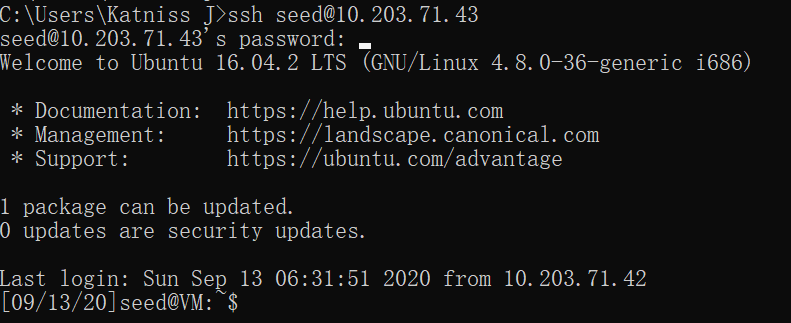
无法连接，攻击成功

SSH服务：

[注]：这个部分写报告时发现做漏了，由于宿主机的Ipv4地址改变，所以重新配置了虚拟机的地址为10.203.71.43，其他部分的虚拟机地址均为10.19.109.160



在用户机器上与服务器建立ssh连接：



连接已建立：



使用netwox 78进行攻击

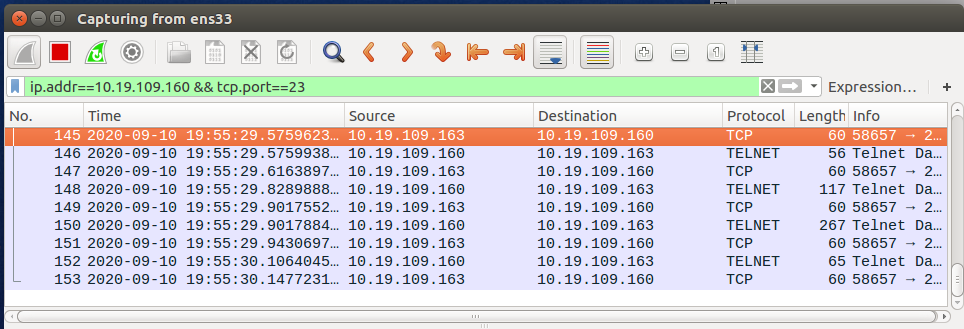


攻击成功

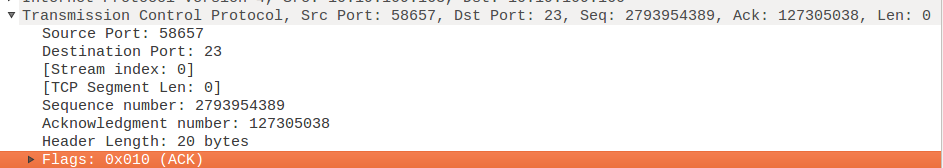


## 3.4 Task 4: TCP Session Hijacking

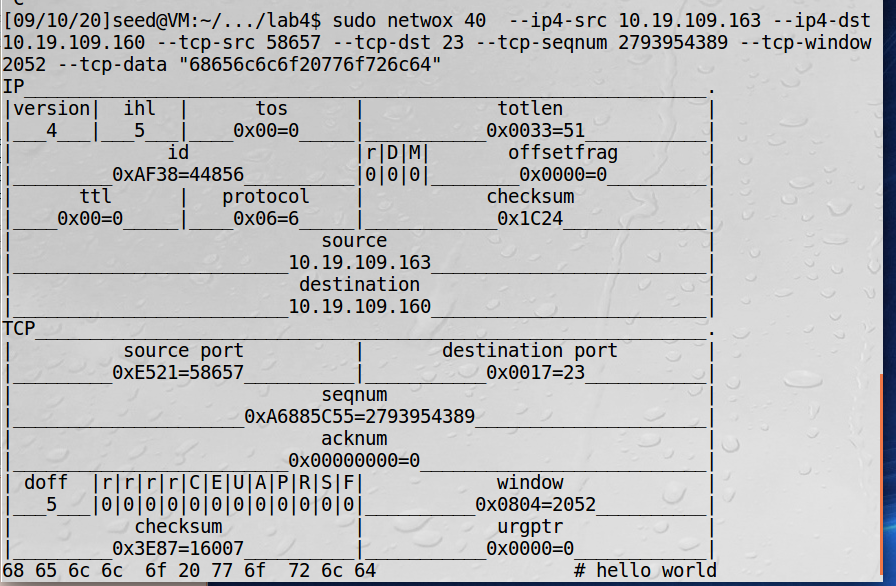
虚拟机地址为原来的10.19.109.160，Telnet远程登录后，使用wireshark抓包



找到最后一条报文中的信息



进行会话劫持



Hello world发送成功

